What is sensitive data at Indiana University?

The following data elements require the highest level of protection. Please note, this is not a comprehensive list, but can be used as a guide for identifying data assigned the restricted and critical data classifications.

FEDERAL AND STATE LAWS

Data that is regulated by Federal or State laws including but not limited to:

- ◊ Family Rights and Privacy Act (FERPA)
- ◊ Health Insurance Portability and Accountability Act (HIPAA)
- ◊ Electronic Communications Privacy Act (ECPA)
- ◊ Payment Card Industry Data Security Standard
- ◊ Gramm-Leach-Bliley Act (GLBA)
- ◊ Freedom of Information Action (FOIA)
- ◊ Federal Trade Commission (FTC) Red Flag Rule (Identity Theft Regulation)
- ◊ Indiana State Data Protection and Security Laws Ind. Code 4-1-10, 4-1-11, 24-4-14

RESTRICTED DATA

Individual Student University Records

- ·Grades/Transcripts*
- ·Courses taken/Schedule
- ·Advising records
- ·Educational services received
- ·Disciplinary actions
- ·Student Financial Aid, Grants, and Loans
- ·Financial account and payment information
- ·Admissions information including test scores, high school GPA, class rank
- ·Personal Restricted Information such as:
  Date of birth, gender, marital status, ethnicity, country of citizenship, visa information, immunization, residency, veteran status, military status, student affiliations, parent information, emergency contact information
- ·Student directory information restricted by student request (FERPA restrictions)

When restricted data is breached, student notice is required.

***Official Transcripts treated as critical data**

CRITICAL DATA

SSN and Other Personally Identifiable Information:

Name (First name or initial and Last name), when stored or displayed with one or more of these data elements:

- Social Security Number
- Driver's license number
- State identification card number
- Financial account numbers such as credit, debit, or bank account numbers
- System Password/PINs
- Identifiable health information

Requires notice to the Indiana Attorney General within 2 business days if information is breached without the necessary encryption. In addition, notification to the student is required. If you suspect data has been breached, contact it-incident@iu.edu.

INQUIRIES?

Contact your Department's IT Security representative to inquire about the security measures that must be implemented for all data that is not considered public. You may also contact the Committee of Data Stewards with questions about data classification.

Handling Sensitive Data

Adhere to these data access principles

•Access data only in the conduct of university business

•Respect the confidentiality and privacy of individuals whose records you access

•Do not access or use IU data for your own personal gain or profit or to satisfy your personal curiosity

•Do not share IU data with third parties unless it is part of your job responsibilities and has been approved by the appropriate data stewards in compliance with IU policies

•Ask questions of your management when you are unsure about data handling procedures

Tips for safeguarding student data

- Know who has access to folders before you save restricted or critical data.
- Do not store sensitive data in locations that are publicly accessible from the Internet. If you can access it without a password, so can others.
- Mobile or portable devices even for email use should be protected by a passcode and encrypted. Laptops, smart phones, and memory sticks can be lost or stolen, and if unencrypted can result in a data breach.
- Follow IU's passphrase requirements and NEVER share your passphrase, use it for other services, or save it in memory!
- If sensitive data is no longer needed, don't retain it! Know your department's retention and disposal policies.
- Be on the lookout for phishing scams. If you receive a suspicious email forward it to phishing@iu.edu.
- Run anti-virus and anti-malware tools routinely and alert IT staff if you encounter issues.

- Do not use unencrypted wireless connections when working with or sending sensitive data.

- Do not send critical data in an email unless the data is encrypted using slashtmp for critical data or CRES.

For more information on safeguarding student data, please visit:https://usss.iu.edu/student-data-mgt/safeguard-data.html

Important to know where to save, how to share, and how to secure sensitive data. All critical data must be encrypted!